

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Makoto MOCHIZUKI, et al.

Application No.:

Group Art Unit:

Filed: October 21, 2003

Examiner:

For: AUTHENTICATION APPARATUS AND COMPUTER-READABLE STORAGE MEDIUM

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-308563

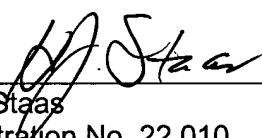
Filed: October 23, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 21, 2003

By: 
H. J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月23日

出 願 番 号

Application Number:

特願2002-308563

[ST.10/C]:

[JP 2002-308563]

出 願 人

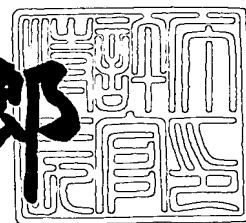
Applicant(s):

富士通株式会社

2003年 4月 8日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3024456

【書類名】 特許願

【整理番号】 0251791

【提出日】 平成14年10月23日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 17/00

【発明の名称】 認証装置及びコンピュータプログラム

【請求項の数】 5

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 望月 誠

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100070150

 【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデンプレイスタワー32階

 【弁理士】

 【氏名又は名称】 伊東 忠彦

 【電話番号】 03-5424-2511

【手数料の表示】

 【予納台帳番号】 002989

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0114942

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置及びコンピュータプログラム

【特許請求の範囲】

【請求項 1】 第 1 の特徴情報を取得する取得手段と、

特徴情報を各ユーザと対応させて登録するデータベースから、該第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出する抽出手段と、

該第 1 の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録する登録手段とを備えたことを特徴とする、認証装置。

【請求項 2】 前記一致の度合いが所定値を超える登録情報の数が一定値以上の場合には、第 2 の特徴情報を読み取るよう促して、読み取られた前記第 2 の特徴情報を前記取得手段により取得する制御手段を更に備えたことを特徴とする、請求項 1 記載の認証装置。

【請求項 3】 個人識別情報及び特徴情報を取得する取得手段と、

登録特徴情報が少なくとも個人識別情報と対応して登録されたデータベースから、該読み取られた個人識別情報に対応する登録特徴情報及び付帯情報を読み出し、該読み取られた特徴情報との一致の度合いを求める手段と、

該読み出された付帯情報で示される個人識別情報に対応する登録特徴情報と、該読み取られた任意のユーザの登録特徴情報との一致の度合いが、いずれも前記求めた一致の度合いより小さい場合に、本人であることを確認する確認手段とを備えたことを特徴とする、認証装置。

【請求項 4】 第 1 及び第 2 の特徴情報を取得する取得手段と、

第 1 及び第 2 の登録特徴情報が、第 1 の登録特徴情報の一致の度合いが一定値を超える所定ユーザに関する付帯情報と共に登録されたデータベースから、該第 1 の特徴情報との一致の度合いが最大値となる第 1 の登録特徴情報に対応する特定付帯情報を抽出する抽出手段と、

該読み取られた第 2 の特徴情報と該特定付帯情報に対応する第 2 の登録特徴情報との一致の度合いが、該読み取られた第 2 の特徴情報と該抽出された付帯情報に対応する第 2 の登録特徴情報との一致の度合いより大きい場合に、ユーザ本人

であることを確認する確認手段とを備えたことを特徴とする、認証装置。

【請求項 5】 コンピュータに認証処理を行わせるコンピュータプログラムであって、

コンピュータに、第 1 の特徴情報を取得させる取得手順と、

コンピュータに、特徴情報を各ユーザと対応させて登録するデータベースから、該第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出させる抽出手順と、

コンピュータに、該第 1 の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録させる登録手順とを行わせることを特徴とする、コンピュータプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、認証装置及びコンピュータプログラムに係り、特に生体情報等の特徴情報を用いて認証、即ち、本人確認を行う認証装置及びコンピュータにそのような認証を行わせるコンピュータプログラムに関する。

【 0 0 0 2 】

本明細書では、生体情報等を含む特徴情報とは、認証（本人確認）に使用し得る指紋パターン、虹彩パターン、血管パターン、音声パターン等の、入力装置により読み取り可能な個人の特徴に関する情報を指す。

【 0 0 0 3 】

【従来の技術】

認証装置には、大略 1 対 1 認証を行う第 1 の方式と、1 対 N（N は 2 以上の整数）認証を行う第 2 の方式とがある。

【 0 0 0 4 】

第 1 の方式では、認証装置に各ユーザの特徴情報が、ユーザを特定可能な個人識別（ID）情報と対応させて予め登録されている。ユーザが本人の ID 情報を入力すると、この ID 情報に対応する登録特徴情報が、読み取られたユーザの特徴情報と比較され、一致の度合いが所定レベルを超えていれば、本人であること

が確認される。所定レベルを高く設定すれば、セキュリティが向上する反面、本人であっても本人であると確認されない確率が増加してしまう。例えば、指紋パターンに関する情報を特徴情報として使用する場合には、本人の指紋パターンが怪我等により特徴情報登録時の指紋パターンと多少異なってしまうことがあり、このような場合には、本人であっても、比較される特徴情報の一致の度合いが低減してしまう。他方、所定レベルを低く設定すると、本人の指紋パターンが怪我等により特徴情報登録時の指紋パターンと多少異なっている場合でも、本人であれば、比較される特徴情報の一致の度合いが増加するものの、他人の類似した特徴情報との一致の度合いも増加してしまうため、セキュリティが低下してしまう。

【 0 0 0 5 】

第 2 の方式では、認証装置に各ユーザの特徴情報が予め登録されている。ユーザの特徴情報が読み取られると、この特徴情報が各登録特徴情報と順次比較され、一致の度合いが所定レベルを超えていれば、本人であることが確認される。この場合、ID 情報の入力是不要であるが、ユーザの数が増大すると、比較処理に時間がかかると共に、類似した登録特徴情報が増大すると、他人と間違えてしまう確率も増加するため、セキュリティが低下してしまう。このため、第 2 の方式は、セキュリティを重視する環境下ではあまり採用されていない。

【 0 0 0 6 】

【発明が解決しようとする課題】

第 1 の方式を採用する認証装置の場合も、第 2 の方式を採用する認識装置の場合も、一番危惧されるのは、他人が本人になりすますことであり、認証精度を向上させて他人が誤って本人と判断されてしまうことを確実に防止することが望まれている。しかし、従来の認証装置では、セキュリティを向上するために認証精度を向上させる、即ち、登録特徴情報の種類を増加させると、比較処理の際に比較すべき項目が増加してしまうので、認証時間が必然的に増加してしまうという問題があった。

【 0 0 0 7 】

又、第 2 の方式を採用する認証装置の場合、ユーザの数が増大して認証精度を

向上させる、即ち、登録特徴情報の数が増大すると、登録特徴情報の種類がたとえ 1 種類であっても、比較処理にかかる時間が増大してしまい、結果的に認証時間が増大してしまうという問題があった。

【 0 0 0 8 】

そこで、本発明は、上記第 1 の方式を採用する場合であっても、上記第 2 の方式を採用する場合であっても、認証時間を増大させることなく認証精度を向上させて、セキュリティの向上を可能とする認証装置及びコンピュータプログラムを提供することを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】

上記の課題は、第 1 の特徴情報を取得する取得手段と、特徴情報を各ユーザと対応させて登録するデータベースから、該第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出する抽出手段と、該第 1 の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録する登録手段とを備えたことを特徴とする認証装置によって達成できる。

【 0 0 1 0 】

上記の課題は、個人識別情報及び特徴情報を取得する取得手段と、登録特徴情報が少なくとも個人識別情報と対応して登録されたデータベースから、該読み取られた個人識別情報に対応する登録特徴情報及び付帯情報を読み出し、該読み取られた特徴情報との一致の度合いを求める手段と、該読み出された付帯情報で示される個人識別情報に対応する登録特徴情報と、該読み取られた任意のユーザの登録特徴情報との一致の度合いが、いずれも前記求めた一致の度合いより小さい場合に、本人であることを確認する確認手段とを備えたことを特徴とする認証装置によっても達成できる。

【 0 0 1 1 】

上記の課題は、第 1 及び第 2 の特徴情報を取得する取得手段と、第 1 及び第 2 の登録特徴情報が、第 1 の登録特徴情報の一致の度合いが一定値を超える所定ユーザに関する付帯情報と共に登録されたデータベースから、該第 1 の特徴情報との一致の度合いが最大値となる第 1 の登録特徴情報に対応する特定付帯情報を抽

出する抽出手段と、該読み取られた第 2 の特徴情報と該特定付帯情報に対応する第 2 の登録特徴情報との一致の度合いが、該読み取られた第 2 の特徴情報と該抽出された付帯情報に対応する第 2 の登録特徴情報との一致の度合いより大きい場合に、ユーザ本人であることを確認する確認手段とを備えたことを特徴とする認証装置によっても達成できる。

【 0 0 1 2 】

上記の課題は、コンピュータに認証処理を行わせるコンピュータプログラムであって、コンピュータに、第 1 の特徴情報を取得させる取得手順と、コンピュータに、特徴情報を各ユーザと対応させて登録するデータベースから、該第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出させる抽出手順と、コンピュータに、該第 1 の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録させる登録手順とを行わせることを特徴とするコンピュータプログラムによっても達成できる。

【 0 0 1 3 】

上記の課題は、コンピュータに認証処理を行わせるコンピュータプログラムであって、コンピュータに、個人識別情報及び特徴情報を取得させる取得手順と、コンピュータに、登録特徴情報が少なくとも個人識別情報と対応して登録されたデータベースから、該読み取られた個人識別情報に対応する登録特徴情報及び付帯情報を読み出し、該読み取られた特徴情報との一致の度合いを求めさせる手順と、コンピュータに、該読み出された付帯情報で示される個人識別情報に対応する登録特徴情報と、該読み取られた任意のユーザの登録特徴情報との一致の度合いが、いずれも前記求めた一致の度合いより小さい場合に、本人であることを確認させる確認手順とを備えたことを特徴とするコンピュータプログラムによっても達成できる。

【 0 0 1 4 】

上記の課題は、コンピュータに認証処理を行わせるコンピュータプログラムであって、コンピュータに、第 1 及び第 2 の特徴情報を取得させる取得手順と、コンピュータに、第 1 及び第 2 の登録特徴情報が、第 1 の登録特徴情報の一致の度合いが一定値を超える所定ユーザに関する付帯情報と共に登録されたデータベー

スから、該第 1 の特徴情報との一致の度合いが最大値となる第 1 の登録特徴情報に対応する特定付帯情報を抽出させる抽出手順と、コンピュータに、該読み取られた第 2 の特徴情報と該特定付帯情報に対応する第 2 の登録特徴情報との一致の度合いが、該読み取られた第 2 の特徴情報と該抽出された付帯情報に対応する第 2 の登録特徴情報との一致の度合いより大きい場合に、ユーザ本人であることを確認させる確認手順とを行わせることを特徴とするコンピュータプログラムによっても達成できる。

【 0 0 1 5 】

従って、本発明によれば、認証時間を増大させることなく認証精度を向上させて、セキュリティの向上を可能とする認証装置及びコンピュータプログラムを実現することができる。

【 0 0 1 6 】

【発明の実施の形態】

本発明の認証装置及びコンピュータプログラムの実施例を、以下に図面と共に説明する。

【 0 0 1 7 】

【実施例】

先ず、本発明の認証装置の第 1 実施例を、図 1 と共に説明する。図 1 は、本発明の認証装置の第 1 実施例を示すブロック図である。認証装置の第 1 実施例では、本発明が、1 台の端末装置（コンピュータ）からなるシステムに適用されている。

【 0 0 1 8 】

図 1 に示す認証装置は、特徴情報読み取り部 9 0、中央処理装置（CPU）9 1、メモリ 9 2、入力装置 9 3、出力装置 9 4、外部記憶装置 9 5、媒体駆動装置 9 6 及びネットワーク接続装置 9 7 を備え、それらはバス 9 8 により互いに接続されている。CPU 9 1、メモリ 9 2、入力装置 9 3、出力装置 9 4、媒体駆動装置 9 6 及びネットワーク接続装置 9 7 等からなる部分は、パーソナルコンピュータ等の周知の汎用コンピュータにより実現できる。即ち、認証装置は、コンピュータにより構成される。

【 0 0 1 9 】

特徴情報読み取り部 9 0 は、周知の方法によりユーザの特徴情報を読み取る構成を有する。本実施例では、説明の便宜上、特徴情報読み取り部 9 0 は、2 種類の特徴情報を読み取る子とが可能なものとする。2 種類の特徴情報は、指紋パターン、虹彩パターン、血管パターン、音声パターン等の生体情報等を含む特徴情報から選択可能である。

【 0 0 2 0 】

メモリ 9 2 は、例えば ROM、RAM 等を含み、本発明のコンピュータプログラムを含む、処理に用いられるコンピュータプログラムと、データとを格納する。CPU 9 1 は、メモリ 9 2 を利用してコンピュータプログラムを実行することにより、必要な処理を行う。

【 0 0 2 1 】

入力装置 9 3 は、例えば、キーボード、ポインティングデバイス、タッチパネル等からなり、ユーザからの指示や情報の入力に用いられる。出力装置 9 4 は、例えば、ディスプレイ、プリンタ、スピーカ等からなり、ユーザへの問い合わせや処理結果の表示の出力に用いられる。

【 0 0 2 2 】

外部記憶装置 9 5 は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置、テープ装置等で構成される。認証装置は、この外部記憶装置 9 5 に、上記コンピュータプログラムとデータを保存しておき、必要に応じて、それらをメモリ 9 2 にロードして使用する。

【 0 0 2 3 】

媒体駆動装置 9 6 は、可搬記録媒体 9 9 を駆動し、その記憶内容にアクセスする。可搬記録媒体 9 9 としては、メモリカード、フロッピー（登録商標）ディスク、CD-ROM、光ディスク、光磁気ディスク等の、任意のコンピュータ読み取り可能な記録媒体が用いられる。ユーザは、この可搬記録媒体 9 9 に上記コンピュータプログラムとデータを格納しておき、必要に応じて、それらをメモリ 9 2 にロードして使用する。

【 0 0 2 4 】

ネットワーク接続装置 9 7 は、LAN やインターネット等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。認証装置は、上記コンピュータプログラムとデータをネットワーク接続装置 9 7 を介して他の装置から受け取り、必要に応じて、それらをメモリ 9 2 にロードして使用する。

【 0 0 2 5 】

図 2 は、図 1 の認証装置にコンピュータプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示す図である。可搬記録媒体 9 9 やサーバ 1 0 0 のデータベース 1 0 1 に保存されたコンピュータプログラムとデータは、メモリ 9 2 にロードされる。このとき、サーバ 1 0 0 は、コンピュータプログラムとデータを搬送する搬送信号を生成し、ネットワーク上の任意の伝送媒体を介して認証装置へ送信する。そして、CPU 9 1 は、そのデータを用いてそのコンピュータプログラムを実行し、必要な処理を行う。

【 0 0 2 6 】

図 3 は、認証装置の登録動作を説明するフローチャートである。同図に示す処理は、図 1 に示す CPU 9 1 が本発明のコンピュータプログラムの第 1 実施例を実行することにより行われる。本実施例では、特徴情報を各ユーザと対応させて登録されるデータベースが、認証装置の外部記憶装置 9 5 等の適切な記憶部内に設けられているものとするが、データベースは、サーバ 1 0 0 側に設けられていても良いことは言うまでもない。

【 0 0 2 7 】

図 3 において、ステップ S 1 では、CPU 9 1 が、例えば出力装置 9 4 にメッセージを表示することでユーザに第 1 の特徴情報の読み取りを促す。ユーザの第 1 の特徴情報（例えば指紋パターン）が特徴読み取り部 9 0 により読み取られ、パラメータが入力されると、CPU 9 1 に通知される。ステップ S 2 では、CPU 9 1 が、データベースをアクセスして、入力された第 1 の特徴情報と類似した特徴情報が登録されているユーザを抽出する。類似した特徴情報とは、第 1 の特徴情報との一致の度合いが所定レベルを超える特徴情報である。ステップ S 3 では、CPU 9 1 が、抽出した類似した特徴情報が登録されているユーザの数が一定値以上であるか否かを判定する。ステップ S 3 の判定結果が YES であると、

ステップ S 4 では、例えば出力装置 9 4 にメッセージを表示することでユーザに上記パラメータを変更して第 1 の特徴情報を再読み取りするよう促して、処理はステップ S 1 へ戻る。これにより、再読み取りされた第 1 の特徴情報が特徴読み取り部 9 0 から CPU 9 1 に入力される。

【 0 0 2 8 】

パラメータは、特徴情報を読み取る際の条件（特徴情報読み取り条件）を示すものであり、例えば指紋パターンを読み取る場合であれば、どの指の指紋であるかを示すものである。従って、最初に右手の親指の指紋パターンを読み取った場合、パラメータを変更して特徴情報を再読み取りする際には、例えば右手の中指又は左手の親指の指紋パターンを読み取れば良い。尚、パラメータとしては、特徴情報を読み取る際の解像度を示すものであっても良い。

【 0 0 2 9 】

ステップ S 3 の判定結果が N O であると、ステップ S 5 では、読み取られたユーザの第 1 の特徴情報を、CPU 9 1 が、上記の如く類似した特徴情報が登録されているユーザに関する付帯情報と共にデータベースに登録する。ステップ S 6 では、CPU 9 1 が、上記の如く類似した特徴情報が登録されているユーザの数が一定値以上であるか否かを判定し、判定結果が N O であると、処理は終了する。ステップ S 6 で用いる一定値は、ステップ S 3 で用いる一定値と同じである必要はなく、例えばステップ S 3 で用いる一定値より大きな値であっても良い。

【 0 0 3 0 】

ステップ S 6 の判定結果が Y E S であると、ステップ S 7 では、CPU 9 1 が、例えば出力装置 9 4 にメッセージを表示することでユーザに第 2 の特徴情報の読み取りを促す。ユーザの第 2 の特徴情報（例えば虹彩パターン）が特徴読み取り部 9 0 により読み取られ、パラメータが入力されると、CPU 9 1 に通知される。ステップ S 8 では、CPU 9 1 が、読み取られたユーザの第 2 の特徴情報を、付帯情報と共に格納されているこのユーザの第 1 の特徴情報と共に、データベースに登録し、処理は終了する。

【 0 0 3 1 】

尚、第 1 の特徴情報と第 2 の特徴情報は、同じ種類の特徴情報であっても、互

いに異なる種類の特徴情報であっても良い。前者の場合、例えば第 1 の特徴情報は右手の親指の指紋パターンで、第 2 の特徴情報は右手の薬指の指紋パターンである。この場合、特徴情報読み取り装置 9 0 の構成が簡単である。又、後者の場合、例えば第 1 の特徴情報は右手の親指の指紋パターンで、第 2 の特徴情報は右目の虹彩パターンである。この場合、特徴情報読み取り部 9 0 は、指紋パターン及び虹彩パターンの両方を読み取るように構成される必要があるが、異なる種類の特徴情報を用いて認証処理を行うので、認証の信頼性は著しく向上する。

【 0 0 3 2 】

次に、図 3 に示す登録処理によりデータベースに登録される情報の形態を、表 1 及び表 2 と共に説明する。

【 0 0 3 3 】

表 1 は、上記第 1 実施例が 1 対 1 認証を行う第 1 の方式に適用された場合のデータベース内の登録情報を示す。この場合、図 3 に示すステップ S 1 の前に、ユーザの個人識別 (I D) 情報の入力促すステップと、入力された I D 情報がデータベースに登録されている場合にのみ処理をステップ S 1 へ進めるステップが設けられることは言うまでもない。

【 0 0 3 4 】

【表 1】

| I D 情報 | 第 1 の特徴情報 | 付帯情報 | 第 2 の特徴情報 |
|-----------|-----------|---------------------------------|-----------|
| I D 0 0 1 | F 1 0 1 | I D 1 0 1, I D 2 0 0 | F 2 0 1 |
| I D 0 0 2 | F 1 0 2 | I D 3 0 1, I D 5 0 3, I D 5 0 4 | F 2 0 2 |
| ... | | | |
| I D X X X | F Y Y Y | I D 1 0 1, I D 3 0 6 | F Z Z Z |

例えば、ユーザの I D 情報が I D 0 0 1 であり、その入力確認されると、このユーザの第 1 の特徴情報 F 1 0 1 と類似する第 1 の特徴情報が登録されたユーザの数が、第 1 の特徴の欄を検索することで抽出される。抽出されたユーザの I D 情報 I D 1 0 1, I D 2 0 0 は、I D 情報 I D 0 0 1 に対する付帯情報の欄に登録される。又、I D 情報が I D 0 0 1 のユーザの第 2 の特徴情報 F 2 0 1 が入力されれば、I D 情報 I D 0 0 1 に対する第 2 の特徴情報の欄に登録される。第

1 の方式の場合、入力された特徴情報は、同じ ID 情報に対して登録された特徴情報とのみ比較されるので、データベースには、ID 情報（ID 情報の欄）が登録されていることが必須である。

【0035】

表 2 は、上記第 1 実施例が 1 対 N（N は 2 以上の整数）認証を行う第 2 の方式に適用された場合のデータベース内の登録情報を示す。

【0036】

【表 2】

| 第 1 の特徴 情報 | 付帯情報 | 第 2 の特徴 情報 | ID 情報 |
|---------------|------------------------------|---------------|----------|
| F 1 0 1 | ID 1 0 1, ID 2 0 0 | F 2 0 1 | ID 0 0 1 |
| F 1 0 2 | ID 3 0 1, ID 5 0 3, ID 5 0 4 | F 2 0 2 | ID 0 0 2 |
| ... | | | |
| F Y Y Y | ID 1 0 1, ID 3 0 6 | F Z Z Z | ID X X X |

例えば、ID 情報が ID 0 0 1 のユーザの第 1 の特徴情報 F 1 0 1 が入力されると、類似する第 1 の特徴情報が登録されたユーザの数が、第 1 の特徴の欄を検索することで抽出される。抽出されたユーザの ID 情報 ID 1 0 1, ID 2 0 0 は、ID 情報 ID 0 0 1 に対する付帯情報の欄に登録される。又、ID 情報が ID 0 0 1 のユーザの第 2 の特徴情報 F 2 0 1 が入力されれば、ID 情報 ID 0 0 1 に対する第 2 の特徴情報の欄に登録される。第 2 の方式の場合、入力された特徴情報は、登録された全ての特徴情報と比較されるので、データベースには、ID 情報（ID 情報の欄）が登録されていることが必須ではないが、比較の結果入力された ID 情報がどのユーザのものであるかを認識可能とするために、ID 情報（ID 情報の欄）が登録されていることが望ましい。

【0037】

図 4 は、第 1 の方式を採用する認証装置の認証動作を説明するフローチャートである。同図に示す処理は、図 1 に示す CPU 9 1 が本発明のコンピュータプログラムの第 2 実施例を実行することにより行われる。

【0038】

図 4 において、ステップ S 1 1 では、CPU 9 1 が、例えば出力装置 9 4 にメ

ッセージを表示することでユーザにID情報の入力を促し、入力装置93から入力されたID情報を取得する。ステップS12では、CPU91が、取得したID情報が表1の如きデータベースに登録されているか否かを判定する。ステップS12の判定結果がNOであると、ステップS22は、ユーザの確認が行えないと判断し、必要に応じて出力装置94にその旨を示すメッセージを表示し、処理は終了する。

【0039】

ステップS12の判定結果がYESであると、ステップS13では、CPU91が、例えば出力装置94にメッセージを表示することでユーザに第1の特徴情報の読み取りを促して、ユーザの第1の特徴情報（例えば指紋パターン）が特徴読み取り部90により読み取られるとCPU91に入力される。ステップS14では、CPU91が、入力された第1の特徴情報と、データベースに登録されているID情報に対応する第1の特徴情報との一致の度合いを示す値を求める。又、ステップS15では、CPU91が、入力された第1の特徴情報と、データベースに登録されているID情報に対応する付帯情報で示されるID情報に対応する第1の特徴情報との一致の度合いを示す値を求める。ステップS16では、CPU91が、ステップS14で求められた値がステップS15で求められた値より大きいか否かを判定する。ステップS16の判定結果がNOであると、他人がユーザ本人になりすましている可能性があるので、処理はステップS22へ進む。

【0040】

ステップS16の判定結果がYESであると、ステップS17では、CPU91が、データベースに第2の特徴情報が登録されているか否かを判定し、判定結果がNOであると、処理は後述するステップS21へ進む。ステップS17の判定結果がYESであると、ステップS18では、CPU91が、例えば出力装置94にメッセージを表示することでユーザに第2の特徴情報の読み取りを促して、ユーザの第2の特徴情報（例えば虹彩パターン）が特徴読み取り部90により読み取られるとCPU91に入力される。ステップS19では、CPU91が、入力された第2の特徴情報と、データベースに登録されているID情報に対応す

る第2の特徴情報との一致の度合いを示す値を求める。ステップS20では、CPU91が、ステップS19で求められた値が予め設定された一定値より大きいかな否かを判定する。ステップS20の判定結果がNOであると、他人がユーザ本人になりすましている可能性があるので、処理はステップS22へ進む。

【0041】

ステップS20の判定結果がYESであると、ステップS21では、CPU91が、ユーザがデータベースに登録されている本人であることを確認し、必要に応じてその旨を示すメッセージを出力装置94に表示した後、処理は終了する。これにより、認証時間を増大させることなく、認証の信頼性を向上することができる。

【0042】

ステップS21で得られた確認結果は、認証装置が適用されているシステムに応じて使用される。例えば認証装置が研究室への立ち入りを許可・禁止するシステムに適用されていれば、ステップS21で得られた確認結果により研究室の鍵が開けられ、研究室への立ち入りが許可される。他方、ステップS22が実行された場合には、研究室の鍵は閉められたままとなり、研究室への立ち入りは禁止される。認証装置が適用されるシステム自体は特に限定されず、例えばコンピュータシステム又は特定の記憶装置へのアクセスを許可・禁止するシステム等にも適用可能である。

【0043】

図5は、第2の方式を採用する認証装置の認証動作を説明するフローチャートである。同図に示す処理は、図1に示すCPU91が本発明のコンピュータプログラムの第3実施例を実行することにより行われる。

【0044】

図5において、ステップS31では、CPU91が、例えば出力装置94にメッセージを表示することでユーザに第1の特徴情報の読み取りを促して、ユーザの第1の特徴情報（例えば指紋パターン）が特徴読み取り部90により読み取られるとCPU91に入力される。ステップS32では、CPU91が、表2の如きデータベースに登録されている第1の特徴情報のうち、入力された第1の特徴

情報との一致の度合いを示す値が最大の第 1 の特徴情報を求める。又、ステップ S 3 3 では、CPU 9 1 が、例えば出力装置 9 4 にメッセージを表示することでユーザに第 2 の特徴情報の読み取りを促して、ユーザの第 2 の特徴情報（例えば虹彩パターン）が特徴読み取り部 9 0 により読み取られると CPU 9 1 に入力される。ステップ S 3 4 では、CPU 9 1 が、入力された第 2 の特徴情報と、ステップ S 3 2 で求めた一致の度合いを示す値が最大の第 1 の特徴情報と共に登録されている第 2 の特徴情報との一致の度合いを示す値を求める。ステップ S 3 5 では、CPU 9 1 が、入力された第 2 の特徴情報と、ステップ S 3 2 で求めた一致の度合いを示す値が最大の第 1 の特徴情報に対応する付帯情報で示される ID 情報に対応する第 2 の特徴情報との一致の度合いを示す値を求める。

【 0 0 4 5 】

ステップ S 3 6 では、CPU 9 1 が、ステップ S 3 4 で求められた値がステップ S 3 5 で求められた値より大きいかな否かを判定する。ステップ S 3 6 の判定結果が NO であると、他人がユーザ本人になりすましている可能性があるので、処理はステップ S 3 8 へ進む。ステップ S 3 8 は、ユーザの確認が行えないと判断し、必要に応じて出力装置 9 4 にその旨を示すメッセージを表示し、処理は終了する。

【 0 0 4 6 】

ステップ S 3 6 の判定結果が YES であると、ステップ S 3 7 では、CPU 9 1 が、ユーザがデータベースに登録されている本人であることを確認し、必要に応じてその旨を示すメッセージを出力装置 9 4 に表示した後、処理は終了する。入力された第 2 の特徴情報は、付帯情報で示される ID 情報に対応する第 2 の特徴情報とのみ比較され、データベースに登録された全ての第 2 の特徴情報と比較されることはないので、認証時間を増大させることなく、認証の信頼性を向上することができる。

【 0 0 4 7 】

ステップ S 3 6 で得られた確認結果は、上述の如く、認証装置が適用されているシステムに応じて使用される。

【 0 0 4 8 】

図 6 は、認証装置の登録監視処理を説明するフローチャートである。同図に示す処理は、図 1 に示す CPU 9 1 が本発明のコンピュータプログラムの第 4 実施例を実行することにより行われる。

【 0 0 4 9 】

図 6 において、ステップ S 4 1 では、CPU 9 1 が、ユーザに登録処理を促すタイミングであるか否かを判定する。ユーザに登録処理を促すタイミングは、例えば一定期間毎、ユーザが登録している第 1 の特徴情報と類似する特徴情報が一定数以上（即ち、一定数以上のユーザ（ID 情報）に対して）データベースに登録された時点等である。ステップ S 4 1 の判定結果が YES になると、ステップ S 4 2 では、CPU 9 1 が、例えば出力装置 9 4 にメッセージを表示することでユーザに図 3 に示す如き登録処理を促し、処理はステップ S 4 1 へ戻る。この場合、登録処理を促されたユーザは、図 3 に示す登録処理をステップ S 7 から開始するようにしても良い。

【 0 0 5 0 】

この登録監視処理を行うことで、既に特徴情報をデータベースに登録済のユーザに対しても、データベースに登録された類似する特徴情報が増加して認証の信頼性が低下するのを防止するための最低限の登録特徴情報の追加を促すことができる。又、ユーザ自身は、特にデータベースに登録された類似する特徴情報を意識する必要がない。

【 0 0 5 1 】

次に、本発明の認証装置の第 2 実施例を、図 7 と共に説明する。図 7 は、本発明の認証装置の第 2 実施例を示すブロック図である。認証装置の第 2 実施例では、本発明が、クライアント・サーバシステムのような、サーバと端末装置（コンピュータ）とがネットワークを介して接続されたシステムに適用されている。認証装置は、サーバにより構成される。

【 0 0 5 2 】

図 7 において、サーバ 5 0 0 及び端末装置 5 1 1 は、ネットワーク 5 2 1 を介して接続されている。サーバ 5 0 0 には、データベースを構成する記憶装置 5 0 1 が接続されている。尚、記憶装置 5 0 1 は、ネットワーク 5 2 1 を介してサー

バ 5 0 0 と接続された構成であっても良い。端末装置 5 1 1 には、特徴情報読み取り部 9 0 が接続されている。ネットワーク 5 2 1 は、有線及び／又は無線のネットワークから構成されている。サーバ 5 0 0 及び端末装置 5 1 1 は、いずれも周知の汎用コンピュータにより構成される。

【 0 0 5 3 】

認証装置の第 2 実施例では、図 3 ～図 6 と共に説明した如き処理がサーバ 5 0 0 側で行われ、サーバ 5 0 0 側が特徴情報読み取り部 9 0 で読み取られた特徴情報がネットワーク 5 2 1 を介して取得し、サーバ 5 0 0 側から端末装置 5 1 1 に対するメッセージをネットワーク 5 2 1 を介して送出する点が、認証装置の第 1 実施例と異なる。

【 0 0 5 4 】

上記各実施例では、データベースには第 1 及び第 2 の特徴情報が登録されているが、第 1 ～第 M (M は 3 以上の整数) の特徴情報を登録するようにしても良いことは、言うまでもない。ただし、M の値が大きくなれば、認証の信頼性は向上するが、認証時間も増加するので、M の値は必要とされる認証の信頼性及び認証速度に応じて適切に決定すれば良い。

【 0 0 5 5 】

尚、本発明は、以下に付記する発明をも包含するものである。

【 0 0 5 6 】

(付記 1) 第 1 の特徴情報を取得する取得手段と、

特徴情報を各ユーザと対応させて登録するデータベースから、該第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出する抽出手段と、

該第 1 の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録する登録手段とを備えたことを特徴とする、認証装置。

【 0 0 5 7 】

(付記 2) 前記一致の度合いが所定値を超える特徴情報の数が一定値を超える場合には、特徴情報読み取り条件を示すパラメータを変更して前記第 1 の特徴情報を再読み取りするよう促して、再読み取りされた第 1 の特徴情報を前記取

得手段により取得する制御手段を更に備えたことを特徴とする、付記 1 記載の認証装置。

【 0 0 5 8 】

(付記 3) 前記一致の度合いが所定値を超える登録情報の数が一定値以上の場合には、第 2 の特徴情報を読み取るよう促して、読み取られた前記第 2 の特徴情報を前記取得手段により取得する制御手段を更に備えたことを特徴とする、付記 1 記載の認証装置。

【 0 0 5 9 】

(付記 4) 前記登録手段は、前記第 2 の特徴情報を前記データベースに登録することを特徴とする、付記 3 記載の認証装置。

【 0 0 6 0 】

(付記 5) 前記第 1 の特徴情報及び前記第 2 の特徴情報は、同じ種類又は互いに異なる種類の特徴情報であることを特徴とする、付記 3 又は 4 記載の認証装置。

【 0 0 6 1 】

(付記 6) 個人識別情報及び特徴情報を取得する取得手段と、
登録特徴情報が少なくとも個人識別情報と対応して登録されたデータベースから、該読み取られた個人識別情報に対応する登録特徴情報及び付帯情報を読み出し、該読み取られた特徴情報との一致の度合いを求める手段と、
該読み出された付帯情報で示される個人識別情報に対応する登録特徴情報と、該読み取られた任意のユーザの登録特徴情報との一致の度合いが、いずれも前記求めた一致の度合いより小さい場合に、本人であることを確認する確認手段とを備えたことを特徴とする、認証装置。

【 0 0 6 2 】

(付記 7) 第 1 及び第 2 の特徴情報を取得する取得手段と、
第 1 及び第 2 の登録特徴情報が、第 1 の登録特徴情報の一致の度合いが一定値を超える所定ユーザに関する付帯情報と共に登録されたデータベースから、該第 1 の特徴情報との一致の度合いが最大値となる第 1 の登録特徴情報に対応する特定付帯情報を抽出する抽出手段と、

該読み取られた第2の特徴情報と該特定付帯情報に対応する第2の登録特徴情報との一致の度合いが、該読み取られた第2の特徴情報と該抽出された付帯情報に対応する第2の登録特徴情報との一致の度合いより大きい場合に、ユーザ本人であることを確認する確認手段とを備えたことを特徴とする、認証装置。

【0063】

(付記8) 前記第1の特徴情報及び前記第2の特徴情報は、同じ種類又は互いに異なる種類の特徴情報であることを特徴とする、付記7記載の認証装置。

【0064】

(付記9) コンピュータに認証処理を行わせるコンピュータプログラムであって、

コンピュータに、第1の特徴情報を取得させる取得手順と、

コンピュータに、特徴情報を各ユーザと対応させて登録するデータベースから、該第1の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出させる抽出手順と、

コンピュータに、該第1の特徴情報を、該特徴情報に関する付帯情報と共に該データベースに登録させる登録手順とを行わせることを特徴とする、コンピュータプログラム。

【0065】

(付記10) コンピュータに、前記一致の度合いが所定値を超える特徴情報の数が一定値を超える場合には、特徴情報読み取り条件を示すパラメータを変更して前記第1の特徴情報を再読み取りするよう促して、再読み取りされた第1の特徴情報を前記取得手順により取得させる制御手順を行わせることを特徴とする、付記9記載のコンピュータプログラム。

【0066】

(付記11) コンピュータに、前記一致の度合いが所定値を超える特徴情報の数が一定値以上の場合には、前記任意のユーザの第2の特徴情報を読み取るよう促して、読み取られた前記第2の特徴情報を前記取得手順により取得させる制御手順を行わせることを特徴とする、付記9記載のコンピュータプログラム。

【0067】

(付記12) 前記登録手順は、コンピュータに、前記第2の特徴情報を前記データベースに登録させることを特徴とする、付記11記載のコンピュータプログラム。

【0068】

(付記13) 前記第1の特徴情報及び前記第2の特徴情報は、同じ種類又は互いに異なる種類の特徴情報であることを特徴とする、付記11又は12記載のコンピュータプログラム。

【0069】

(付記14) コンピュータに認証処理を行わせるコンピュータプログラムであって、

コンピュータに、個人識別情報及び特徴情報を取得させる取得手順と、

コンピュータに、登録特徴情報が少なくとも個人識別情報と対応して登録されたデータベースから、該読み取られた個人識別情報に対応する登録特徴情報及び付帯情報を読み出し、該読み取られた特徴情報との一致の度合いを求めさせる手順と、

コンピュータに、該読み出された付帯情報で示される個人識別情報に対応する登録特徴情報と、該読み取られた任意のユーザの登録特徴情報との一致の度合いが、いずれも前記求めた一致の度合いより小さい場合に、本人であることを確認させる確認手順とを備えたことを特徴とする、コンピュータプログラム。

【0070】

(付記15) コンピュータに認証処理を行わせるコンピュータプログラムであって、

コンピュータに、第1及び第2の特徴情報を取得させる取得手順と、

コンピュータに、第1及び第2の登録特徴情報が、第1の登録特徴情報の一致の度合いが一定値を超える所定ユーザに関する付帯情報と共に登録されたデータベースから、該第1の特徴情報との一致の度合いが最大値となる第1の登録特徴情報に対応する特定付帯情報を抽出させる抽出手順と、

コンピュータに、該読み取られた第2の特徴情報と該特定付帯情報に対応する

第 2 の登録特徴情報との一致の度合いが、該読み取られた第 2 の特徴情報と該抽出された付帯情報に対応する第 2 の登録特徴情報との一致の度合いより大きい場合に、ユーザ本人であることを確認させる確認手順とを行わせることを特徴とする、コンピュータプログラム。

【 0 0 7 1 】

(付記 1 6) 前記第 1 の特徴情報及び前記第 2 の特徴情報は、同じ種類又は互いに異なる種類の特徴情報であることを特徴とする、付記 1 5 記載のコンピュータプログラム。

【 0 0 7 2 】

以上、本発明を実施例により説明したが、本発明は上記実施例に限定されるものではなく、種々の変形及び改良が可能であることは、言うまでもない。

【 0 0 7 3 】

【発明の効果】

本発明によれば、認証時間を増大させることなく認証精度を向上させて、セキュリティの向上を可能とする認証装置及びコンピュータプログラムを実現することができる。

【図面の簡単な説明】

【図 1】

本発明の認証装置の第 1 実施例を示すブロック図である。

【図 2】

図 1 の認証装置にコンピュータプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示す図である。

【図 3】

認証装置の登録動作を説明するフローチャートである。

【図 4】

第 1 の方式を採用する認証装置の認証動作を説明するフローチャートである。

【図 5】

第 2 の方式を採用する認証装置の認証動作を説明するフローチャートである。

【図 6】

認証装置の登録監視処理を説明するフローチャートである。

【図 7】

本発明の認証装置の第 2 実施例を示すブロック図である。

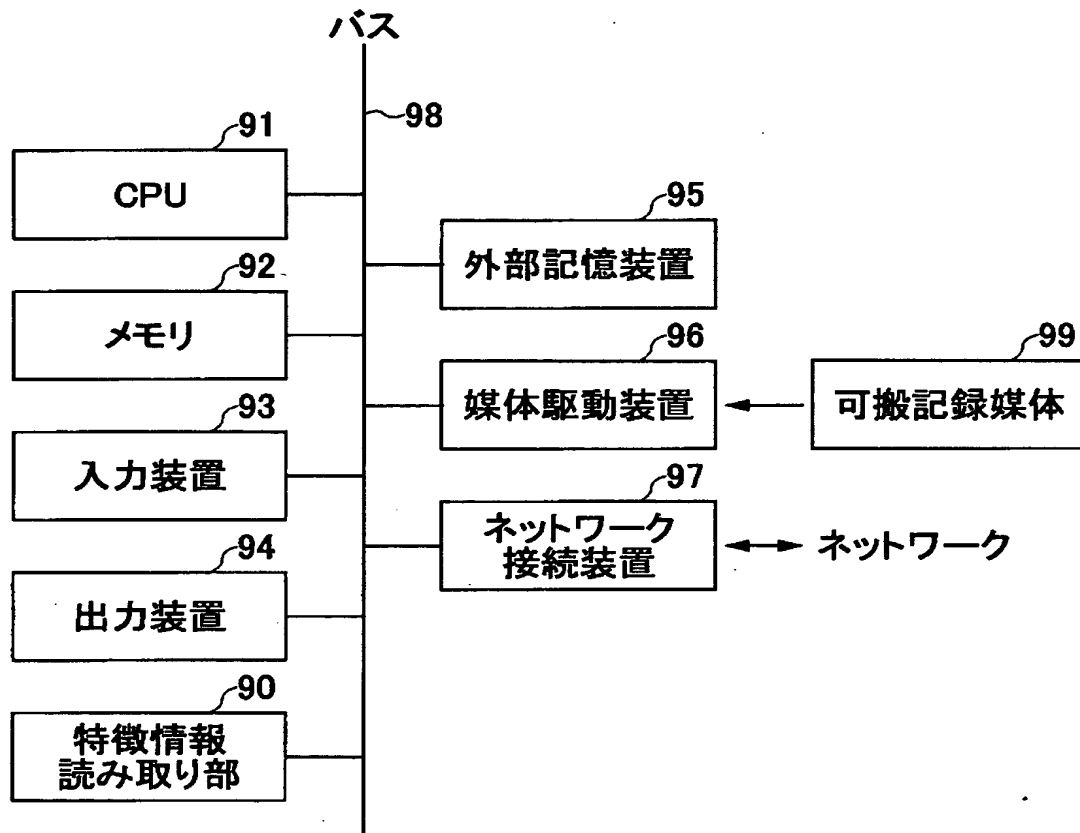
【符号の説明】

| | |
|-------|------------|
| 9 0 | 特徴情報読み取り部 |
| 9 1 | C P U |
| 9 2 | メモリ |
| 9 3 | 入力装置 |
| 9 4 | 出力装置 |
| 9 5 | 外部記憶装置 |
| 9 7 | ネットワーク接続装置 |
| 9 9 | 可搬記録媒体 |
| 5 0 0 | サーバ |
| 5 0 1 | 記憶装置 |
| 5 1 1 | 端末装置 |
| 5 2 1 | ネットワーク |

【書類名】 図面

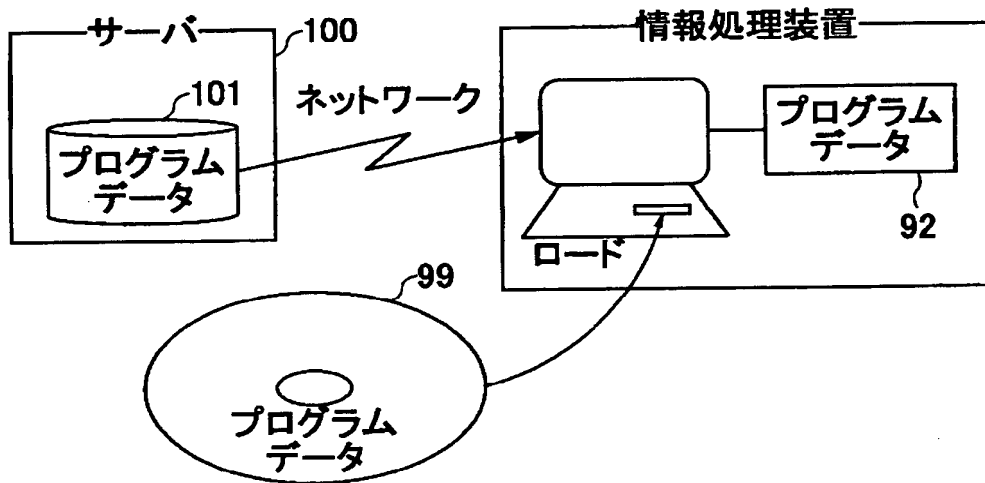
【図 1】

本発明の認証装置の第1実施例を示すブロック図



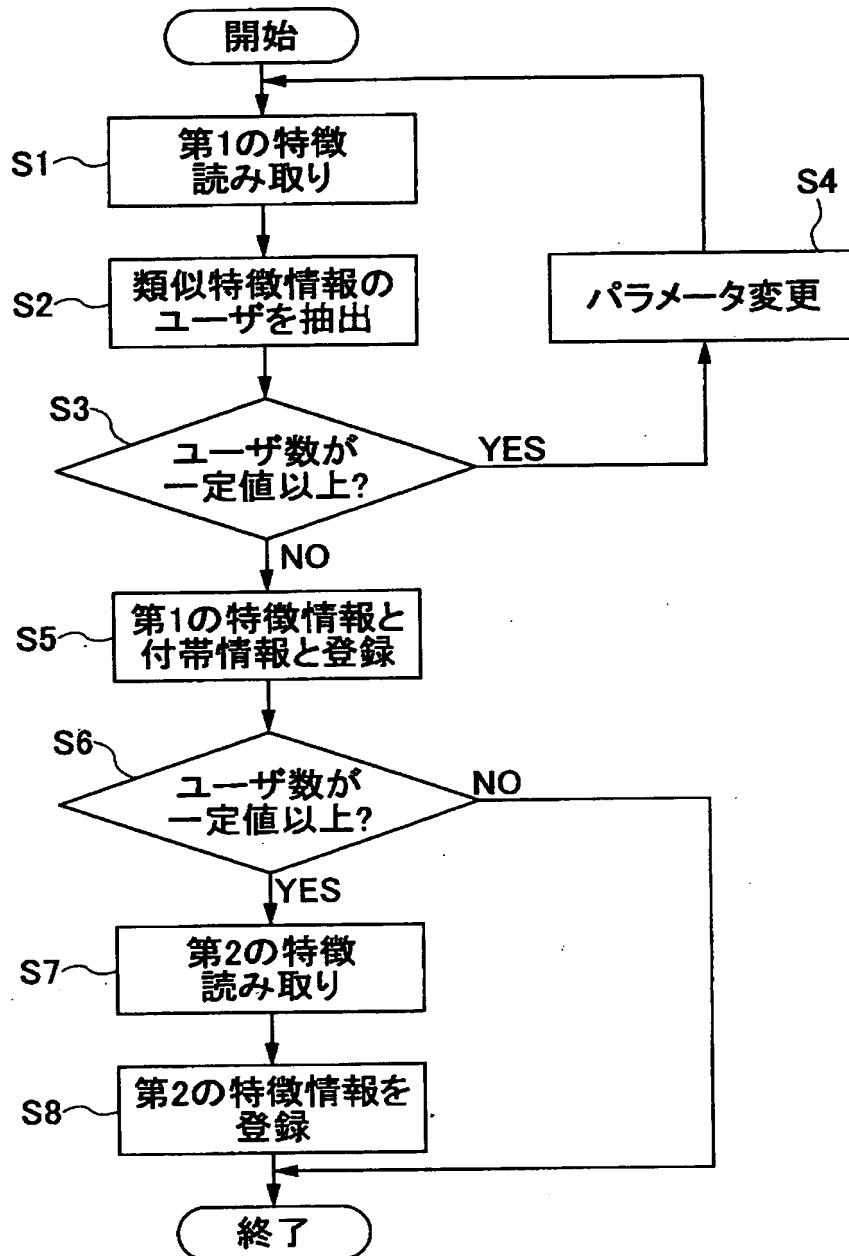
【図 2】

図 1 の認証装置にコンピュータプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示す図



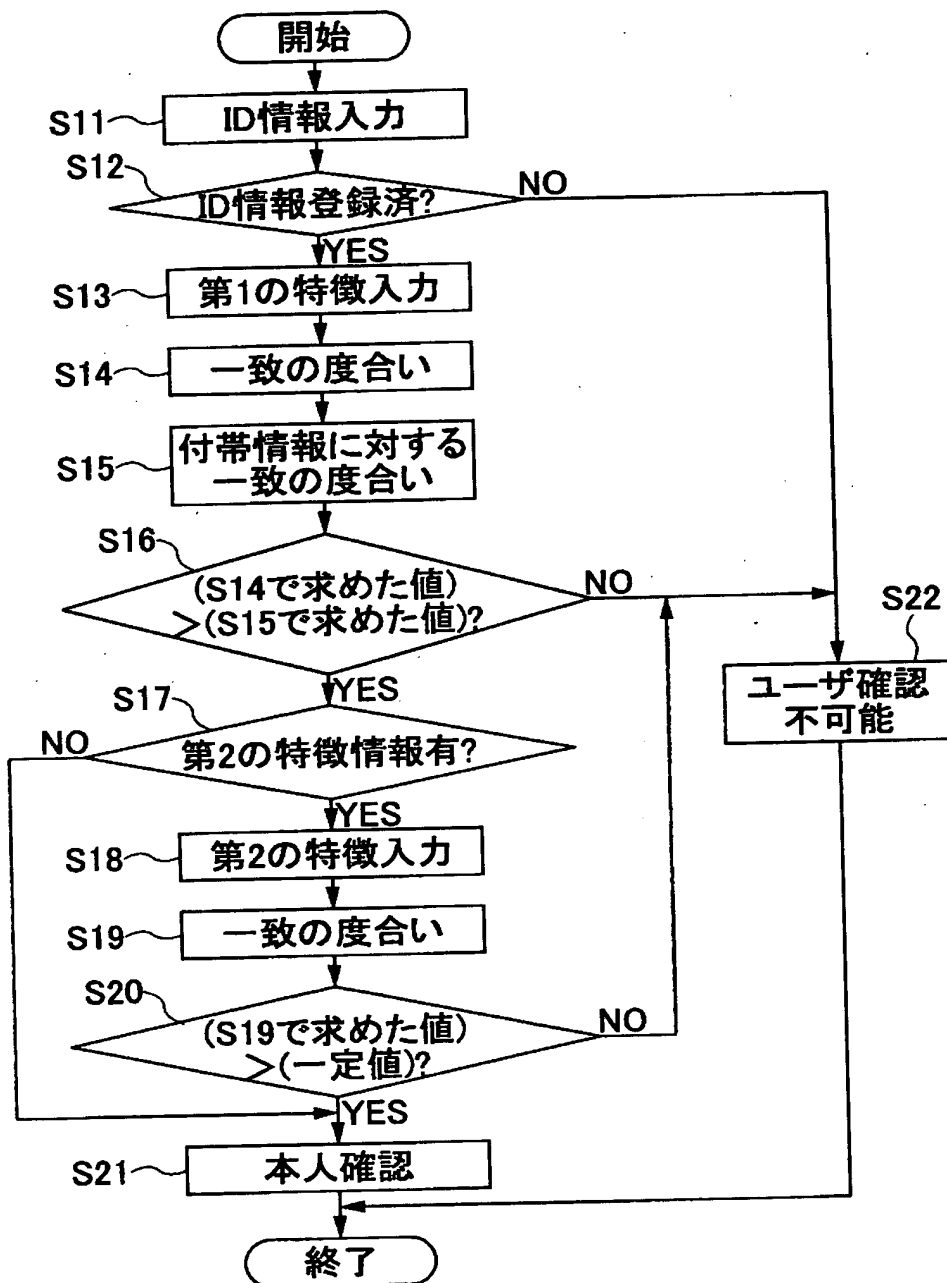
【図 3】

認証装置の登録動作を説明するフローチャート



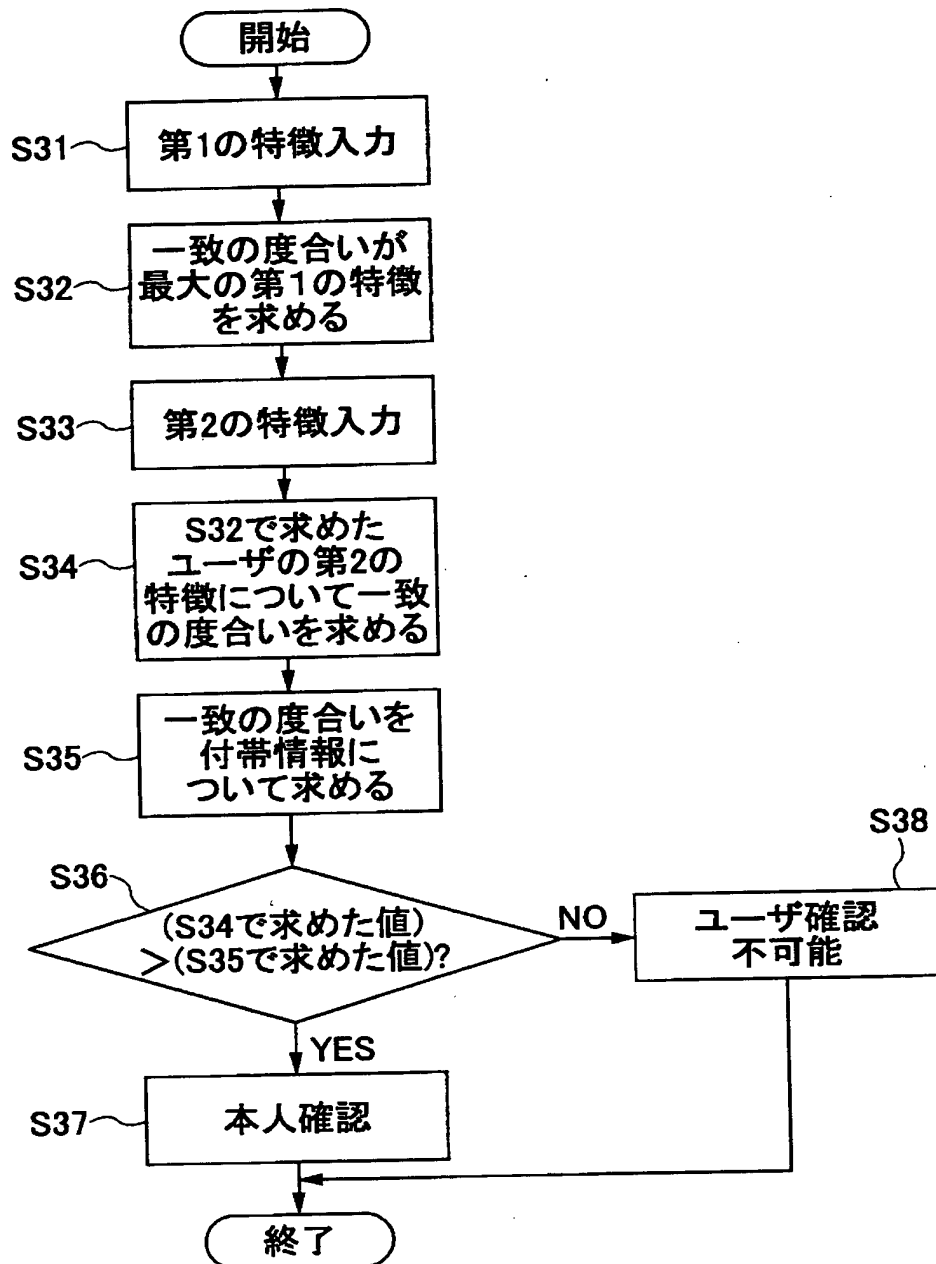
【図 4】

第1の方式を採用する認証装置の
認証動作を説明するフローチャート



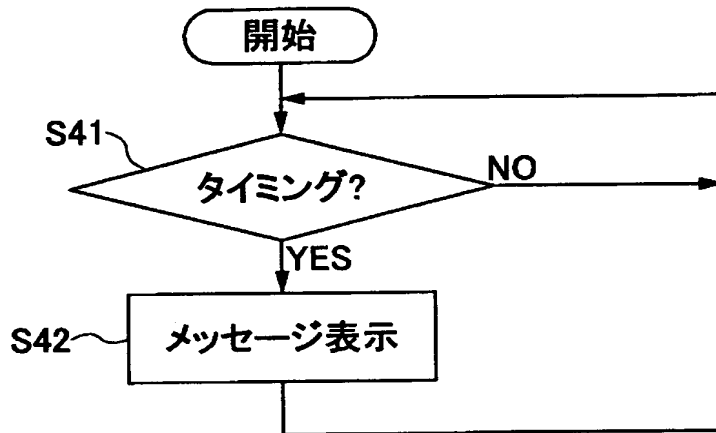
【図 5】

第2の方式を採用する認証装置の
認証動作を説明するフローチャート



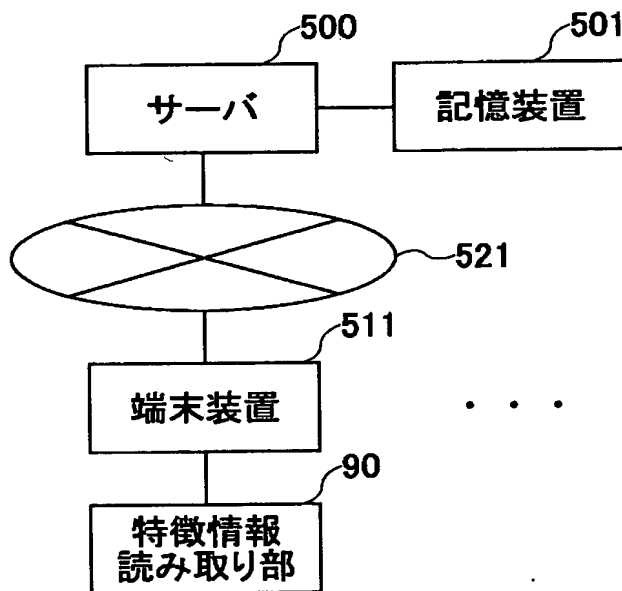
【図 6】

認証装置の登録監視処理を説明するフローチャート



【図 7】

本発明の認証装置の第2実施例を示すブロック図



【書類名】 要約書

【要約】

【課題】 本発明は認証装置及びコンピュータプログラムに関し、認証時間を増大させることなく認証精度を向上させて、セキュリティの向上を可能とすることを目的とする。

【解決手段】 第 1 の特徴情報を取得する取得部と、特徴情報を各ユーザと対応させて登録するデータベースから、第 1 の特徴情報との一致の度合いが所定値を超える特徴情報に対応するユーザを抽出する抽出部と、第 1 の特徴情報を、特徴情報に関する付帯情報と共にデータベースに登録する登録部とを備えるように構成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社